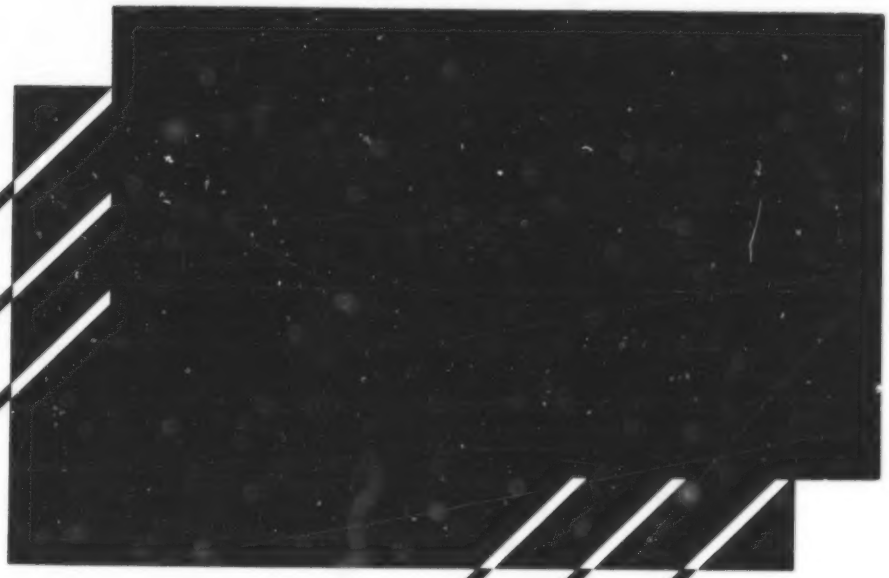
Gouvernement du Canada
Ministère des Communications

Government of Canada
Department of Communications

Le Centre canadien de recherche sur l'informatisation du travail
Canadian Workplace Automation Research Centre



Canada

DATA SECURITY IN OFFICE AUTOMATION

AN EXPLORATORY STUDY OF ISSUES AND CONCERNS ARISING OUT OF THE OFFICE COMMUNICATIONS SYSTEMS (OCS) PROGRAM

by Dr. Jake V. Th. Knoppers
Senior Guest Researcher

Canadian Workplace Automation Research Centre

First published, August, 1984. Revised and reissued for the International Electronic Information Forum. Montreal, June, 1987. The opinions expressed in this report are those of the author.

DOC-CWARC-87-E-C03

90-05470//

PREFACE

This report is an slightly edited version of an earlier report prepared by Dr. Knoppers for the Department of Communications in August, 1984. It has been reissued with some additional information because the findings of the earlier report remain valid.

The original report was the result of a series of studies undertaken by INFOMAN INC. on data security issues arising from office automation. These studies were commissioned by the Security Programs and Operations Division, Department of Communications, as an activity parallel to and in support of the Office Communications Systems (OCS) program.

The purpose of these studies was to rationalize a major concern in the development of new technologies for office automation, and to bring to the attention of the public and private sector the need to address a potential problem area in the introduction of these new technologies. As such, this report should be of assistance not only in the work carried out as part of the development and introduction of office automation systems in particular but also in the use of integrated information systems in general.

A "Post Scriptum" has been added to include recent developments and activities related to security matters which should be of interest to readers of this report.

Finally, it should be noted that a companion report titled Legal Issues arising out of Integrated Information Systems: An Overview of Practical Considerations and Recent Developments is also being made available as part of the International Electronic Information Forum.

TABLE OF CONTENTS

		Page
I.	EXECUTIVE SUMMARY	1
II.	INTRODUCTION	5
	A. BACKGROUND	5
	B. PURPOSE AND SCOPE	6
	C. METHODOLOGY	7
III.	THE OFFICE COMMUNICATIONS SYSTEM (OCS) PROGRAM	10
	A. PURPOSE	10
	B. SCOPE AND INFORMATION CONTENT	10
	C. ISSUES AND CONCERNS DISCUSSED WITH OCS STAFF	13
IV.	DATA SECURITY REQUIREMENTS FOR INFORMATION UNDER THE CONTROL OF THE FEDERAL GOVERNMENT	16
	A. LEGISLATION AFFECTING DATA SECURITY IN OFFICE AUTOMATION	16
	1. Introduction	16
	2. Access to Information Act	16
	3. Privacy Act	17
	4. Official Secrets Act	18
	5. Criminal Code	18
	6. Evidence Act	19
	B. INFORMATION MANAGEMENT CONSIDERATIONS	20
	1. Introduction	20
	2. Government Policy for the Protection of Information	20
	3. Information Management Policy	21
	C. OBSERVATIONS ON DATA SECURITY REQUIREMENTS IN OFFICE AUTOMATION IN THE FEDERAL GOVERNMENT	25
V.	THE PRIVATE SECTOR AND DATA SECURITY REQUIREMENTS IN OFFICE AUTOMATION	32
VI.	CONCLUSIONS AND RECOMMENDATIONS	36
VII.	POST SCRIPTUM	42
REFERENCES		46

I. EXECUTIVE SUMMARY

The federal government is currently supporting a series of field trials in the use of office automation technologies called the Office Communication Systems (OCS) program. Administered by the Department of Communications, the main purpose of the OCS program is to "provide Canadian high tech industries an opportunity to demonstrate their capability in office automation and consequently stimulate Canadian development". Another very important objective of the program is to address questions and concerns related to the introduction of office automation in the workplace such as ergonomics, quality of work, organizational impacts and other human/social factors.

There are five field trials in the OCS program. These trials involve data, voice, graphics, text and video transmissions via telephone, cable and fibre optics as well as the introduction of multifunction workstations. The basic approach of the trials is the integration of computer and communications technologies to perform various information handling tasks in support of managerial and administrative functions. One of the concepts includes, wherever feasible, the replacement of existing hard-copy based information technologies (paper, microfilm, copier, facsimile transmission, etc.) The emphasis of the current field trials has been on making the technologies work and on finding appropriate ways for workers to adapt to and use office automation systems. Consequently, information management considerations in general, and data security issues in information access and use in particular, have not been a major concern and therefore have not yet received the attention they deserve.

This report represents an initial study of data security issues and concerns, particularly those related to sensitive information of a non-national security nature, arising out of the introduction of office automation systems in the federal government. The study is based on interviews with those involved in the field trials in a managerial role; and analysis of existing and draft federal government legislation policies, directives and guidelines for the management and protection of information; and, review of existing literature as well as the author's own previous work in information management, Access to Information and Privacy legislation and the vulnerability of computer/communications systems.

Hightlights or key elements of the interviews with the managers and other officers of the OCS field trials revealed that:

- the current applications are basically in the financial and administrative areas and generally do not involve sensitive information although uncertainty exists regarding the scope of what constitutes sensitive information;

- once users become familiar with office automation technologies, they will naturally tend to use them to handle all types of information including information relating to national security or otherwise sensitive information;

- retrofitting protective measures at a later date is an expensive and difficult task;

- data security requirements should be built into office automation systems early in the design and development stage;

- greater awareness of the need to protect certain types of information is needed particularly since a wave of new and more sophisticated users is anticipated in the future; and,

Federal legislation affecting security, confidentiality, privacy, and current and new administrative policies of the federal government on the use of information technologies and in information management, including those arising from the Access to Information and Privacy Acts, are noted, paying particular attention to those in the data security area. A preliminary review from a data security perspective makes it clear that these requirements apply also to information handled by office automation systems. The report notes that office automation systems and accompanying procedures must be able to meet legal and federal administrative information policy requirements on information access and use if they are to be used in as wide a range of application areas as possible.

The report puts forward the argument that the size of the office automation market and its penetration by Canadian suppliers is directly related to the ability of such systems to handle sensitive information. This is especially true where office automation systems are used to increase the effectiveness of decision-making by senior management as differentiated from utilizing such systems as productivity tools in the handling of administrative or routine information flows.

As such, the study points out, in a preliminary fashion, the link between the needs of the federal government and private sector for office automation systems to be able to handle sensitive information. The study makes the point that inclusion of data security considerations in the offerings of Canadian suppliers should increase both the value and market penetration of office automation products in the Canadian market and abroad.

Finally, the report makes the recommendation that consideration be given to:

- the preparation of a set of practical guidelines and procedures for applying existing legal and administrative requirements on access to and use of information under the control of the federal government to office automation systems;

- conducting a pilot project, possibibly using a field trial administered by DOC, to address in a practical sense data security issues and concerns arising from the use of office automation systems; and,

- developing for Canadian suppliers a set of documents which would, in practical terms, state clearly the data security requirements that office automation systems in the federal government would have to meet and to what degree these are analogous to the needs of the private sector.

II. INTRODUCTION

A. BACKGROUND

The Department of Communications is coordinating a number of field trials in office automation. This initiative in office automation is called the Office Communications Systems (OCS) program. The OCS field trials consist of testing different combinations of equipment made by Canadian suppliers in various areas of application in a select number of government agencies. The field trials involve graphics, voice, data, video and text transmissions via telephone, cable and fibre optics as well as the concept of multifunction workstations.

The OCS concept is both one of integrating computer/communications/-information (CCI) technologies and of replacing existing hard-copy based information technologies (paper, microfilm, copier, facsimile transmission, etc.). The primary focus, so far, in the OCS field trials has been on the technology itself as well as quality of work, ergonomics and other human/social factors.

On 1 July 1983, the Access to Information Act and the Privacy Act (ATIP) became law. This legislation is, in effect, a new information handling policy for the federal government. It is technology-independent, i.e. it applies equally to all forms of recorded information under the control of federal government institutions, and sets forth criteria and conditions under which information may or may not be disclosed.

Policies and regulations also exist in the federal government which provide for the protection of certain information against unauthorized disclosure. Many of the new restrictions on access to information and protection of personal information have been added to existing government policies and regulations.

A basic question arising as a result of the OCS program and office automation in general is, "How does one apply the new information policy (ATIP) to developments in information technology (informatics) such as OCS?" and in particular, "How does one address concerns arising from the use of these technologies in the federal government and as it relates to the objectives of the OCS program in support of private sector development?" The approach to office automation is one where there is no longer a central MIS or records office gatekeeper. It is to be used by all, in a user-friendly mode. It is portable. It mixes elements of records, EDP, word processing, and telecommunications management, each with its own set of procedures and practices.

In the context of the above factors, the Security Programs and Operations Division, Department of Communications, asked Infoman Inc. to undertake a study of data security issues arising from office automation. As such, this report should be of assistance in the work carried out under the OCS program and, possibly, to organizations responsible for direction and guidance in information management.

B. PURPOSE AND SCOPE

The objective of this report is to identify data security issues arising from office automation in the federal government and to identify, in a preliminary fashion, parallel or ensuing issues in the private sector. The report does not address the issue of information of a national security nature as measures to protect this type of information are already prescribed.

Other security issues which may relate to the increasing use of high technology, such as protection of equipment against misuse or theft are not addressed in this study. Nevertheless, such issues are important and will need attention to ensure availability of equipment as integral and essential components of the automated office.

The scope of the report is threefold and is reflected in the three chapters which follow. Firstly, this study involved an analysis of the existing field trials in terms of area of application, information content and discussion/interviews with field trial participants. Secondly, existing, new and draft legislation, government security and information management policies and related materials pertinent to office automation and data security issues and concerns are reviewed. And thirdly, since the purpose of the field trials is to assist Canadian suppliers services, a preliminary discussion on the links between data security requirements of the federal government and those of the private sector was undertaken.

C. METHODOLOGY

The work consisted primarily of:

- reviewing the current field trials in office automation in the federal government in relation to:
  - the objectives of the Office Communications Systems (OCS) program,
  - the application areas and information content of field trials,
  - interviews with field trial managers and others on data security concerns arising from office automation;
- reviewing current requirements within the federal government, including key current and anticipated federal legislation, which require that information of a certain nature receive appropriate protection when processed, stored or transmitted electronically so that required confidentialities are maintained; and,

- identifying, in a preliminary fashion, security and confidentiality requirements of the private sector in office automation which are similar in nature (or function) to those of the federal government.

The study is entitled "Data Security". The term encompasses the concepts of "security", "confidentiality" and "privacy", all of which have a wide variety of meanings in both a broad context and a narrow technical sense.

It therefore might be useful to briefly outline the meanings of the terms or concepts of "security", "confidentiality" and "privacy" in relation to office automation and information management and in the context of this report:

security - This is neither a question of physical security of computers, communication and other equipment nor one of access to buildings and offices. Rather, the term refers to the logical security measures which ensure that only those authorized can access the office automation system and the information contained therein. As such, "security" refers to the control of access to information and the procedures required to protect against unauthorized disclosure, destruction or manipulation of data. Typical security measures of this nature include sign-on controls, access codes, call-back, encryption, etc., i.e. software and system features.

confidentiality - This terms embodies the requirements that rules on disclosure and non-disclosure of specific and identifiable entities of recorded information are adhered to. In short it refers to the requirement to protect data against unauthorized disclosures. The "need to know" principle is very much a part of confidentiality. The requirements to keep certain information confidential, laid down in law and government policy, take place at various levels and in various contexts, i.e. public vs government only, department only, Cabinet only, third-party confidences, a specific group of individuals involved in a particular program (e.g. Census, Income Tax) or new policy development, etc.

Confidentiality requirements can be based on position of the creator of the document, level of activity or information content, etc., or any combination of these.

privacy - In its proper context and under the new Privacy Act, privacy refers to a certain set of rules pertaining to the creation, processing, transmission, access and use, protection and destruction of recorded information on or about individuals. It also refers to accuracy and confidentiality requirements of data pertaining to an individual, the right of access by an individual to such data and the assurance that data utilization rules are adhered to. Privacy is a relatively new concept and has emerged as a new human right in response to the emerging information age.

It should be noted that the explanations of these three terms are only provisional. Further work needs to be done in defining these terms both in concept and practice. This is especially true for the rather new concept of "data integrity". Consequently, in this report, the term "data security" is used as a collective term as it is premature to state at this time whether a particular issue, concern or requirement in office automation is one of security, confidentiality, privacy or data integrity or any combination of these.

III. THE OFFICE COMMUNICTIONS SYSTEMS (OCS) PROGRAM

A. PURPOSE

The Office Communication Systems (OCS) program is an initiative in office automation in the federal government administrated by the Department of Communications through the launching of a series of field trials. The purpose of the OCS field trials is to "provide Canadian high tech industries an opportunity to demonstrate their capability in office automation and consequently to stimulate Canadian industrial development". One of the major aims of the OCS program is thus "to enable the Canadian Office Automation Industry to put itself in a position to satisfy the huge potential market in Canada and abroad".

A second major purpose of the OCS program is user acceptance of multi-function workstations in their office or workspace. Consequently, a considerable secondary effort in the OCS program is taking place in addressing questions and concerns related to ergonomics, organizational factors and productivity.

B. SCOPE AND INFORMATION CONTENT

Approximately $12 million of federal funds have been allocated to support the field trials in office automation. Most of these funds have been allocated to the supply of various combinations of hardware, software, telecommunication facilities, etc. by Canadian suppliers at five test sites. Remaining funds are being used to support the field trials and to conduct studies addressing issues such as systems performance, user acceptance, human/social factors, organizational questions and productivity.

Field trials are taking place in the following departments:

- Department of National Defense
  (Financial Services Branch, Ottawa and Winnipeg);
- Environment Canada
  (Environment Protection Services and Management Services, Ottawa/-Hull and regions);
- Revenue Canada (Customs and Excise)
  (Tax Interpretation Group and Senior Management, Ottawa/Hull and Toronto);
- Energy, Mines and Resources
  (Administrative Services and Personal, Ottawa); and,
- Communications Canada
  (Broadcast and Social Policy Branch and Minister's Office, Ottawa).

The area of application in the field trial of the Department of National Defense is the Financial Services Branch while the users are to be officers in the financial policy and procedures area at National Defense Headquarters in Ottawa and at both the Air Command Headquarters and Canadian Forces Base in Winnipeg. The information content relates basically to financial policy and financial administration. The emphasis is on electronic mail, scheduling of tasks, document creation and filing, indexing and retrieving information and spreadsheet usage. The system is already being used for electronic messaging between Ottawa and Winnipeg concerning errors in transactions relating to the payroll and automatic payment of bills.

In Environment Canada the first phase of the field trial is taking place in two areas: namely,

- the department's Management Services Directorate; and,
- the Environmental Protection Service.

The emphasis is electronic mail and messaging, voice communications, word processing, activity management and electronic file management. The basic intent is to let users adopt the system for whatever purpose they find useful. In the Environmental Protection Service, the system is intended to be used by senior and middle management, while in the Management Services Directorate the emphasis is on use by middle and junior management as well as administrative and support staff.

At Revenue Canada (Customs and Excise), the area of application of the OCS field trial is that of senior management officers in Excise in Ottawa and Toronto of both the Tax Interpretation Group and a management group. The emphasis here is on providing integrated voice and data services, advanced telephony, text messaging and document processing. In terms of information content, this is mainly current tax interpretations, documentation supporting office procedures, forms creation and routing as well as calendars and daily schedules of participants. One objective of the trial is to provide individual online access to legal databases.

The focus of the field trial at Energy, Mines and Resources is that of electronic retrieval and filing in the Finance and Administration Branch. The basic information content of this OCS application is the department's Administrative Policy Manuals.

At the Department of Communications, the area of application of OCS is the Broadcast and Content Services Policy Branch in the Policy Sector as well as the offices of the Minister, Deputy Minister and Senior Assistant Deputy Minister. While specific attention is being paid to electronic mail and ministerial correspondence, other functions include word processing, Telidon, spreadsheets, communications and remote terminal access to central file servers.

In summary, the OCS field trials are concentrating on assessing the technical problems of using various mixes of Canadian supplied components and on studying specific issues related to the introduction of new information technologies and systems into the workplace. The main areas of application are electronic mail and messaging, calendering and scheduling, word processing, spreadsheet, administrative and financial policies and procedures, etc. The planned information content in the current field trials thus tends to be mostly of an administrative nature. However, the field trial at Revenue Canada (Excise) includes the participation of the Tax Interpretation Group and the field trial at DOC focuses on expediting ministerial correspondence, Treasury Board submissions, reports and policy analysis, etc. In EMR, the field trial consists specifically of information which is open to the public with direct online access to the stand-alone system being envisaged.

In several trials, the decision was taken that no sensitive or classified information would be handled by the OCS prototypes. However, it is anticipated that as users become more familiar with their office automation systems they will gradually tend to maximize the use of these systems and will want the ability to handle all types of information.

C. ISSUES AND CONCERNS DISCUSSED WITH OCS STAFF

As part of the interviews with project managers and other officers associated with the field trials, a number of topics were discussed concerning data security features or requirements applicable to or resulting from office automation. The following is a summary of these topics:

- Basically, all field trials have access and sign-on controls. In addition, there are provisions for distinguishing between "public" or coporate files or documents, including central records, and "private" or personal documents, i.e. one's own desk drawer. Most field trials do not have separate access controls or security levels at the file or document level. An exception so far is

Environment Canada where for the field trial the system is being designed with access controls to be available at the data element level.

- Several respondents noted that from a data security perspective, it may not be possible to do part of one's job one way and another part another way, i.e. once people become familiar in the use of office automation technologies and start to rely on them for their daily work, a tendency develops to utilize the same technology to handle both non-sensitive and sensitive information. The experience with word processing was cited as an example.

- In the past, part of the security features with hard-copy or paper records lay in "volume" and "physical restrictions", i.e. it would take an unauthorized person quite some time to go through all the documents in a filing cabinet to find something of interest and one would be noticed doing this. With user-friendly office automation technologies and systems, a whole new level of risk and vulnerability has arisen due to the ability to use these systems to search very large volumes of documents for "interesting" information very quickly or from a remote location without being noticed. One could possibly copy documents without them ever being checked out from a records office or being "missed" from the file. It may also be possible to alter documents electronically without leaving the same evidence of modification as for paper records.

- System dependency - If office automation is successful and the parallel paper system is dropped, does one do a daily backup copy? What if someone corrupts the system? What if an electronic document is misfiled? In a hard-copy based system one will eventually see a misfile and correct it; in an office automation system, if there is a "misfile", the document could be permanently lost.

- Those familiar with computer/communications systems noted that retrofitting one's office automation system to meet various levels of data security standards is tremendously expensive in terms of dollars, person years and time. It may not even be possible for certain systems' designs. They were of the opinion that data security issues should be addressed and covered from the beginning in an office automation system, i.e. in the planning, design, testing and implementation stages.

- On a more general note, the fact that a whole wave of sophisticated users is about to enter the government workforce, coupled with the increasing user-friendliness and portability of office automation systems and equipment, was both a cause for concern and a reason to provide for data security policies and procedures in office automation systems including consideration of what constitutes un-ethical behaviour.

IV. DATA SECURITY REQUIREMENTS FOR INFORMATION UNDER THE CONTROL OF THE FEDERAL GOVERNMENT.

A. LEGISLATION AFFECTING DATA SECURITY ISSUES IN OFFICE AUTOMATION

1. Introduction

This section presents a preliminary review, from the perspective of office automation, of key current and anticipated federal legislation and pursuant regulations which require that information of a certain nature receive appropriate protection when handled electronically so that required confidentiality is maintained. Examples of federal laws which require that access to specific recorded information be restricted and that confidentiality be maintained include the Income Tax Act, Statistics Act, Canada Pension Plan Act, Criminal Records Act, and the Family Allowances Act. It is not the purpose of this chapter to focus on legislation particular to a certain government agency or program but rather on those which apply to all government agencies and thus to any application of office automation. Consequently, the key Acts are:

- Access to Information Act
- Privacy Act
- Criminal Code
- Official Secrets Act
- Evidence Act

2. Access to Information Act

This act, which became law 1 July 1983, gives Canadians the right of access to information under the control of the federal government including that in machine-readable form. This means that any information or possible combinations of data that can be derived from an office automation system is subject to the Act.

However, the Act outlines several areas where information is exempted from disclosure or where disclosure is subject to review before disclosure. Through its exemptions and providing for restrictions on disclosure of certain information, the Act presents a set of criteria for determining what data security concerns must be addressed.

As a result of the Access to Information Act, there is now a legal requirement that government data security measures support the intent of this Act and be in harmony with it.

3. Privacy Act

The Privacy Act is a revised and expanded version of the Canadian Human Rights Act, Part IV. The definition of personal information has been expanded and some of the rights clarified. The Act became law 1 July 1983.

Basically, privacy rights require that information on, about or linked to individuals be timely, accurate and relevant; that such personal information is destroyed when no longer needed; that information collected or stored on individual be limited, have a clear purpose or use and be collected directly from the individual wherever possible; that individuals have a right to know what data exists on themselves, who collects, uses and/or stores such data; that individuals have a right of access (with specific exemptions) to their personal information, be able to review the same as to its accuracy and relevancy and to request deletion, addition and/or correction; and that in case of dispute there is a right of appeal to a neutral third party, i.e. the Privacy Commissioner, etc.

As such, the Privacy Act, like the Access to Information Act, sets forth criteria for access, use and confidentiality of information on individuals including that held in any office automation system. In short, any office automation system used by a federal institution which carries personal information must be able to ensure that the legal requirements of the Privacy Act can be supported.

4. Official Secrets Act

Until the enactment of the Access to Information and Privacy Acts, the Official Secrets Act was the only law of general applicability on which government regulations and policies were based which sought to ensure that information which should not be disclosed, was not. The Act also requires that public servants take an oath of secrecy. However, for the present and immediate future, it appears that Access and Privacy legislation are more predominant in determining broad as well as detailed security criteria for information in office automation systems. Further, the Official Secrets Act looked at security of information primarily from a national security interest perspective. The Access to Information Act contains a number of access restrictions, both discretionary and mandatory, for categories of information not necessarily of "national security interest" but still "sensitive" to unauthorized, premature or uncontrolled disclosure.

5. Criminal Code

On 7 February, 1984 an ommibus bill to make amendments to the Criminal Code, Bill C-19, was tabled in the House of Commons. Of interest to this study are two proposed amendments pertaining to computer crime and data abuse. If these amendments become law, the use of computer/communications technologies and other integral components of office automation for sensitive data will be protected by law.

In the context of office automation in particular and computer/communications in general, data security procedures need to be developed to ensure that if and when breaches occur, especially in the disclosure of sensitive information, one might be able to lay a charge under the Criminal Code irrespective of Access or Privacy legislation.

This would require, at the least, being able to demonstrate that the user of an office automation system was fully aware and had been fully briefed as to what constitutes "criminal" behaviour in the use of office automation systems. This will also require the development of a very clear set of user instructions regarding the use of office automation systems including specific technical and procedural measures to ensure that users are both aware of data security requirements and have been trained in their implementation. If this is not done, it may be difficult to litigate when the proposed amendments on computer crime and data abuse become law.

It should be noted that under ATIP legislation and Treasury Board Policy, the disclosure of classified information and sensitive information in response to an access request is not a chargeable offense under the present Official Secrets Act. However, recourse to the proposed new sanctions under the Criminal Code on data abuse might still be possible if office automation systems were involved in the unauthorized disclosure of sensitive or personal information and if the user of such systems had been made aware as to what constitutes "unauthorized behaviour".

6. Evidence Act

It is acknowledged that one reason many organizations are hesitant to convert fully to office automation is the uncertainty surrounding the admissibility of computer-generated records as evidence in court. Consequently, any change in the law of evidence which would allow for the admissibility of records generated by office automation systems, including those generated in response to litigation, would remove a serious roadblock in the drive towards greater use of office automation systems in a much wider number of possible application areas.

Currently, Bill S-33, the proposed new Uniform Evidence Act, represents an attempt to bring the laws of evidence in tune with modern information technologies through a new section on recorded evidence which would allow for the admissibility of computer-generated records in the courts. When passed, it should greatly accelerate the trend to office automation systems, especially in the private sector, thereby increasing both the size and scope of this market in Canada. An important ramification of this proposed legislation is that such a change in the Evidence Act will also require that office automation systems be able to demonstrate the integrity of the data in question.

B. INFORMATION MANAGEMENT CONSIDERATIONS

1. Introduction

The purpose of this section is twofold. It focuses on current government policies on protection of information and aso reviews information management policies, directives and guidelines of the federal government. It pays particular attention to those policies which touch on data security concerns and the question of their application or relevance to office automation.

2. Government Policy for the Protection of Information

The policy for the security of information in the federal government is stated in the publication titled "Security of Information in the Public Service of Canada", first issued in 1956 by the Privy Council of Canada with minor revisions in 1977-78. The purpose of this document was to introduce a uniform approach to the identification, classification and protection of classified government information and, most importantly, to ensure that all public servants are made aware of these requirements and would act accordingly. The document sets forth a four-level classification system and set of procedures to be followed to ensure that an

appropriate level of security is maintained to protect information according to its value to a foreign power and the degree of damage or injury that unauthorized disclose would cause to the nation.

While some of the concepts of this security policy may still be valid, there are questions as to its applicability to office automation and the document is considered by many to be inadequate in light of modern security concerns and new information technologies. It should be noted, however, that information classified as being vital to national security interests cannot be processed, transmitted or otherwise handled electronically without special protective measures to protect against compromising emanations and to guard against unwanted monitoring. It was for these reasons that such information was not included in any of the field trials.

Nevertheless, the need remains for office automation systems to process classified information at various and appropriate levels of data security. This is especially true in those areas where office automation systems are to be used to increase the effectiveness of decision-making by senior management (as differentiated from productivity increases in the administrative areas).

3. Information Management Policy

Insofar that office automation represents an attempt at the integration of hitherto separate information technologies, it was deemed worthwhile to briefly review the various "Information Management" chapters in the Treasury Board's Administrative Policy Manual (APM) which contain sections which would be of use in identifying data security concerns arising from office automation.

In order to assist government institutions in implementing and administrating Access to Information and Privacy legislation, and under the authority of the same law, Treasury Board issued, in June 1983, an Interim Policy Guide: Access to Information and Privacy Acts

(Chapter 410, APM). This chapter explains the legal requirements of these acts and prescibes practices which government agencies must follow to be in compliance with these requirements.

From a data security perspective, this policy guide sets out the basis for applying exemptions which govern the refusal of access to government records and protection of personal information and the use and disclosure of the same. The policy guide makes it clear that the Access to Information Act in stating what information should not be disclosed or might be disclosed has in effect become a new framework in which information should be organized and data security concerns addressed.

Part III (Privacy) of the Interim Policy Guide is issued under the authority of both the Privacy Act and the Financial Administration Act. The basic purpose of this policy is the protection of privacy in terms of both the collection, retention and disposal as well as the use and disclosure of personal information. Personal information is defined basically as any recorded information relating to, or which would identify, an individual. The need therefore arises to incorporate the general principles of the Privacy Act, i.e. accuracy, relevance, completeness and timeliness, including appropriate data security procedures within office automation technologies to support the implementation of this policy directive.

Whereas, Chapter 410 presented policy directives and guidelines on access and use of information, chapters in the 430, 440 and 450 series address themselves to the use of information technologies.

Chapters 435 and 436 deal with the use of telecommunication technologies within the federal government. In particular, they outline policies and procedures for the management, administration and acquisition of telecommunications goods and services, and establish responsibilities and requirements for the protection of national security and other sensitive information.

Chapter 440 deals with policies and procedures for electronic data processing (EDP). This chapter was last amended and revised in December 1978 and applies to "all electronic data processing equipment, services and personnel which are used for general purposes in the government". While this chapter does not refer specifically to office automation, the principles expressed therein are applicable. The Chapter recognizes the "ever increasing dependence on computer-based information systems" and directs that the actual management of EDP within departments be based on common planning and procurement, including consideration of security and control practices and mechanisms. Section 8 of the chapter deals specifically with EDP security and forms a key policy component for data security issues in office automation and a directive in this section requires government institutions to ensure that information in their custody in whatever form is protected to the level required by the relevant security classification or degree of sensitivity.

These chapters, although issued some time ago, provide to some extent for the possibility of developments such as office automation; and, the fact that quite often computer policies and telecommunication policies should not be addressed as separate areas but as integrated policies. The policies contained in these chapters seem to have already recognized the need for data security and as a result require that appropriate considerations, especially those of a technical nature, must be taken into account when office automation systems are being installed in federal government institutions.

Finally, there are a series of chapters which deal with the management of recorded information. Of these, Chapter 460 addressed the question of the management of hard-copy records, i.e. the management of physical entities on which information is recorded, while the draft Chapter 461 relates to the management of data, i.e. the management of information irrespective of the physical medium on which it may be recorded.

Chapter 460 was revised and reissued by Treasury Board in March 1983 and is "the first in a series of information policies aimed at assisting departments and agencies in implementing access and privacy legislation". One of the main objectives of this chapter is to ensure that "records are protected from unauthorized access, disclosure and alteration, and from destruction and loss". The chapter deals with the management of the records of a minister's office including both personal and institutional records. It requires that in any record-keeping system:

- the institutional records be included as a subset of the subject file classification system of the institution; and,

- the institutional records be segregated from the minister's personal records.

This policy chapter also requires that "cabinet confidences" form a distinct subset of information and "shall be protected from unauthorized access in accordance with procedures supervised by the Cabinet Documents Security Auditor at the Privy Council Office and, with respect to Treasury Board documents, by the Office of the Secretary of the Treasury Board".

Chapter 461 on the Management of EDP Data is being proposed to replace the old Chapter 440.7 EDP: Records Management. Chapter 461 currently exists in draft form only and is intended to cover the management of information recorded in a form and manner suitable for communication, interpretation or processing by automatic means. The draft document requires government institutions to develop internal procedures to more specifically govern matters such as:

- the protection of personal information, i.e. privacy;
- the classification of machine-readable data in accordance with the injury likely to result from the disclosure of the data;
- the storage, handling, transmission, transfer and destruction of security-classified machine-readable information; and,
- the declassification of security-classified data.

C. OBSERVATIONS ON DATA SECURITY REQUIREMENTS IN OFFICE AUTOMATION IN THE FEDERAL GOVERNMENT

It is clear that Access to Information and Privacy legislation, pursuant regulations, TBC directives and administrative policy apply to information handled via office automation systems. Also, it is emphasized that these requirements apply particularly to all newly recorded information and new systems based or computer/communication/information technologies. New information policies provide for the first time a clear legal framework and criteria for granting and restricting access to government information.

In fact, the statutory responsibilities for controlling access and use of sensitive information are now very clear.

If one of the goals of office automation is to support and increase the effectiveness of decision-making, senior management must be able to use such systems. Therefore, office automation systems will also have to be able to handle the security requirements pertaining to ministerial records, Cabinet documents and "confidences of the Queen's Privy Council".

Of particular interest in the context of office automation are the requirements that:

- Cabinet confidences must be clearly stamped as such by the author;
- Cabinet confidences must be segregated from other records on the same subject;
- a separate record must be kept of those files known to contain Cabinet confidences to ensure their removal in the event of examinations of the files by individuals not authorized to have access to such records; and,
- file jackets or wallets containing any such Cabinet confidences must be clearly marked on the outside as containing Cabinet confidences.

These requirements have been implemented for hard-copy records through the use of physically segregated files and filing systems, special colour-coded file folders, the stamping of individual documents, etc. If office automation systems are to contain records of this kind, and they most certainly will have to if they are to be an effective decision-making support tool for senior management, they will have to meet these operational and data security requirements.

In this context, it should also be noted that a substantial number, if not most, of "Cabinet confidences" do not concern national security but relate to domestic (national, regional and local) economic, social and cultural policies, programs and initiatives and associated disbursements of federal funds (e.g. a regional incentive of work program, a cultural initiative, proposed changes to the Criminal Code relating to divorce, etc.) Therefore, an important question that must be addressed is, "How does one 'distinguish' and 'segregate' confidences of Cabinet, as required under Access to Information regulastions, in office automation systems and protect such records from inadvertent or unauthorized disclosure?"

While current security policies and practices which apply to telecommunications, EDP, word processing, records and data management, etc. do not specifically address office automation systems, the same principles apply. The basic problems that arise, however, are:

a) which combinations of existing policies, guidelines and procedures are particularly relevant to office automation and how can they be applied?; and,

b) what new data security issues and concerns are raised by office automation and what is the best way to address these issues and concerns?

Examples of particular problems which may arise from office automation and data security concerns are: "Will users be able to freely purge and remove files? At what point does a 'draft' become a record of the government and require approval for destruction? At the time a record is created and filed in an office automation system, even if only as a draft, is that not the time that data security considerations come into play?", etc.

In records management terms, a file is basically a container for a group of records while in office automation terminology, a file or filename is often assigned to a single record (e.g. document, letter, report, etc.). Similarly for paper records, security practices work basically at the "records" or "documents in a file" level using specially marked file folders which can, and often do, contain a mix of classified and non-classified information. The principles and practices of the way classified information is readily identified at the file folder and/or document level for hard-copy records will need to be translated into guidelines and practices for office automation systems. It would be useful to identify the interrelationships between records management and office automation as well as the links to data security considerations under Access and Privacy legislation.

Government information management policy (Section 460.6.5) on essential records requires institutions to store a set of essential records at secure sites administrated by the Public Archives. For paper records, this can include microfilms and for traditional or large data processing operations, periodic back-up tapes and data base dumps.

However, the question arises as to how these requirements are to be applied to office automation? Office automation systems are envisaged as very dynamic systems as far as changes in information content are concerned and consist of various hardware/software/data structures and configurations. Office automation systems present a challenge in the area of essential records.

Government records management policy also states that the establishment and application of records schedules is to be done at the file (folder) level. In office automation systems, it may be more practical to do the security classification and declassification, scheduling and disposal, etc. at the "document" level or even at the data element level using strict control rules comparable to those which exist currently in manual operations.

In addition, Section 440.8.5.6 states that "the originator of the data to be processed should determine and clearly indicate the security classification of data" where required. In the context of office automation this would include a facility whereby a user can tag documents of files to indicate the degree of security required as well as the necessary software and other technical features to support a particular application. At some point in time, this may also include a user being able to switch to or invoke a more secure mode in an office automation system. Similarly, the control measures for data input, processing, output, etc. for office automation systems should include appropriate data security components.

The review of existing government policy for the protection of information and current security procedures for classified information in hard-copy form led to a number of specific observations in relation to office automation and data security concerns. It might be userful to cite a number of these in this report. Some examples are:

- In the area of declassification and the fact that material is often time-sensitive, will the use of office automation systems enable one to automatically downgrade documents after expiry of a given period of time, a certain date or the occurence of a specific event?

- In a paper mode, copies of a classified document are often numbered. In an office automation system, how does one prevent unauthorized off-screen copying? Will only certain users have access to decryption programs?

- How does the concept of "sealed" and use of double sealed envelopes translate into an office automation system? Or that of a signed receipt of a document? And signature verification?

- How will the requirements that combinations for padlocks on filing cabinets be changed every six months, with the departure of staff or when combinations are compromised, be implemented on office automation systems (e.g. Will access codes or passwords be changed every six months?) On what intervals should user profiles be reviewed? Will one have to change the passwords of all those tied to an employee's departure, such as when a secretary or administrative officer serving several people leaves?

- How will the "need-to-know" principle be implemented in an office automation system? Should it be built into the user's access profile? Or a document access profile?

- Will the portability of microcomputers and diskettes lead to officers taking classified information home with them?

- How does the requirement that all classified material must be securely locked away at night relate to an office automation application which is available online 24 hours a day? With remote or from-the-home access? Or if resident on unremovable media?

- On the question of carrying classified material home in locked containers, does this translate into some lockable diskette carrying pack? And what about the requirements for the checking in and out of such classified materials? How is this to be reconciled with the goal of office automation systems to offer online access from any telephone anywhere in Canada (or in the world)?

With respect to user awareness and user training in the area of data security in office automation, a strategy based on analogies to hard-copy records might be the most productive. Since the purpose of office automation is that it be user-friendly and thus non-technical, the human aspect of ensuring the protection of sensitive information privides the greater challenge.

Finally, data security requirements in office automation systems will have to take into account existing security policies such as the policy on the classification of documents, letters, working notes, rough sketches, etc. The analogy here is that classification policy applies to all forms of recorded information even though the definition is geared towards hard-copy records. In terms of office automation systems, one question that may be asked is "How does the classification policy apply to rough working drafts of 'electronic documents' or information stored in a person's private file'?"

The combination of current government security policies and of the Access to Information and Privacy Acts would seem to generate two basic categories of information classifications for information protection purposes. One would be the traditional area of information relating to the "national interest" and defence of the nation where cost considerations and possible decrease in operational efficiency of restrictive access measures are secondary to ensuring that required data security levels are maintained. The second would be information whose public release would adversely affect the interest of the party concerned (e.g. government, corporations, and individuals). One could call this "sensi-

tive" information. This is actually a new category brought about due to the discretionary exemptions under Access and Privacy legislation and the introduction of the legal concept of balance and injury tests. One possibility that could be explored in the use of office automation systems in the federal government is to make a clear distinction between those systems which can support the stringent security requirements for information vital to the national interest and those which can support the less stringent security needs for "sensitive" information.

V. THE PRIVATE SECTOR AND DATA SECURITY REQUIREMENTS IN OFFICE AUTOMATION

The main reason for the OCS program is to assist Canadian manufacturers to develop and field test various configurations of office automation systems to put Canadian industry "in a more competitive position to satisfy the huge potential market in Canada and abroad". Questions were raised, however, in the course of this study as to whether the federal government in general and the five field trials in particular can be considered representative of private sector requirements for the electronic office of the federal government are relevant to the private sector.

It should be stated at the outset that there are two key differences between the federal public sector and the private sector as far as data security requirements are concerned.

Firstly, in the federal government there do exist information and accompanying automated support systems which must be protected from unauthorized disclosure "regardless of the cost" because vital national interests are involved. However, this a highly specialized sub-market in computer/communications/information technologies and falls outside the general market for office automation equipment. Although a need exists for this technology in both the public and private sectors, this report does not address this area other than in general terms as already discussed.

Secondly, federal government institutions are obliged to comply with legislation which mandates that certain rules on access, use, disclosure and protection of specific categories of recorded information must be followed, i.e. compliance with Access to Information and Privacy legislation. With respect to this govsernment requirement and its relevance to the private sector, it should be noted that information legislation already exists in a number of European countries which also applies to the private sector, i.e. privacy laws. Further, Canada has now formally

agreed to adhere to the OECD Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data. These guidelines include encouraging all public and private sector organizations to adopt voluntarily the OECD privacy code, i.e. privacy rights for information on individuals held by an organization. In fact, a number of Canadian companies have already adopted privacy rights as part of their corporate policy. Notable examples are IBM, various insurance companies, and recently the Royal Bank. Further, it is estimated that well over 100 U.S. multinationals already have or are in the process of implementing the OECD privacy code. It should be noted that privacy requirements are really both a subset of good information management practices in general, i.e. timely, accurate and relevant information, and data security procedures in particular, i.e. protection of personal information against unauthorized access and disclosure. Consequently, any office automation system in the federal government which can meet the data security requirements of the Privacy Act should be more marketable not only in Canada but also abroad. In summary, in light of trends in the information policy environment, it can also be argued that a product offering which supports privacy rights would give the suppliers a distinct marketing advantage since few, if any, products do so at present.

Further analogies can be made between data security requirements of federal institutions and the private sector. It should be noted that the purpose of office automation is not only productivity increases but also improved decision-making. Of particular importance here is the potential value of office automation to senior management in an organization, i.e. key information being readily available at all times regardless of where one is, to minimize delay and time wastage in communications, etc. In this context, one can argue that similartities do exist between the functional requirements and relationships of senior bureaucrats and the Minister of a government department, and senior management and the president of a company.

For example, the development of a major government policy initiative over a period of time with a critical launch window involves a limited number of key people in different locations in Ottawa, and possibly across Canada, who must be able to communicate information in the form of draft documents, opinions, etc., while being assured of certain levels of information security. This is not unlike a situation in a company where one may be working on a major deal, a change in company direction, a takeover, etc. Quite often code words are used, different combinations of people are involved (and therefore all others must be excluded from access to the information), the documentation (paper and electronic) must be kept segregated, etc. In short, access to information legislation as well as the segregation between the records of a department and those of the office of the Minister, the distinction between regular records and confidences of Cabinet, etc., are all data security requirements which the private sector also has need of, especially if senior management wishes to rely on and have full confidence in an office automation system. In a nutshell, these requirements consist of a matrix of the ability to provide various levels of protection for basic information units in an "electronic filing cabinet" and for various (often changing) combinations of individuals on a need-to-know basis.

At the daily or operational level in the federal government, there are also similarities between the requirements of the Access to Information Act and private sector needs. Examples of "sensitive" information which requires protection are trade secrets, product development information, financial data including budget planning, investigations (internal), strategies and tactics for launching a new policy or new product or service, institutional reorganization, career planning, etc. The basic difference here between the protection of "sensitive" information in the federal government and the private sector is that for the former these requirements are derived from legislation or overall government direction while in the private sector the implementation of such features is more dependent on cost trade-offs and threat-analysis. Consequently, office automation systems developed to meet the requirements of the

Access to Information and Privacy Acts, government information management policies on ministerial records, confidences of Cabinet, those for general government information protection, etc., with such data security features already built-in should be much more marketable in the private sector, especially in view of the fact that retrofitting such features on a system is very expensive and may fall outside the cost-risk analysis of a company.

The above statements should be considered as preliminary comments only since a more thorough review of data security needs of the private sector was well beyond the scope of this study. Nevertheless, it is true, even leaving aside national security considerations, that currently the federal government has data security requirements more stringent than those of the private sector. However, for some of these requirements, there is an international trend to also have them in the private sector (e.g. privacy), while for others there are direct analogies between the functional requirements of federal government agencies and those of the private sector. If the purpose of the OCS field trials is to serve as a testbed for office automation product development to meet the needs of the market place, inclusion of data security considerations in such products should increase both the value and marketability of such products in the Canadian market and abroad.

VI. CONCLUSIONS AND RECOMMENDATIONS

The current field trials in office automation under the Office Communications Systems (OCS) program focus on the development and integration of Canadian computer and telecommunications equipment and associated software. Consequently, the primary emphasis in the field trials has been on making the different components communicate together and the software operational. A second major focus of the field trials is on user acceptance of "multifunction workstations" in their office or workplace and on addressing questions and concerns related to ergonomics and other social factors. It is therefore not surprising that information management issues in general and data security questions in particular were not primary considerations when the field trials were first established.

Consideration appears to have been given to data security in some field trials, although on the whole, there seems to be little awareness of the broad spectrum of data security issues and concerns and especially of what constitutes "sensitive" information as distinct from information directly pertaining to national security. A decision was made at the onset of some field trials that OCS systems in their formative stage should not be used for handling "sensitive" information. However, those in charge of the field trials did recognize that if and when OCS moves out of this first phase, data security concerns would have to be addressed and form part of the decision of whether or not and how OCS is going to be utilized on an on-going basis. While there are no definite plans on how and where the OCS field trials should be expanded of placed on an on-going operational footing, there does seem to be receptiveness towards addressing data security issues.

The information content of the field trials appears to be concentrated in the administrative rather than operational and policy areas of government, i.e. information flows relating to personnel, financial and administrative data and messaging. A notable exception is in DOC where the areas of application are the policy sector and ministerial correspondence as well as document flows in and out of the Minister's Office. These are typical areas where data security concerns are most likely to arise.

Apart from certain privacy issues, there seems to be a general lack of user awareness of the need for data security in general and its practical application to office automation systems in particular. There is widespread agreement and recognition that one of the key issues, if not the key issue, is that of user awareness and user education regarding data security. Specifically, it is in the area of non-national security levels of information and the protective requirements that apply to "sensitive" information where the misunderstandings or lack of awareness form the greatest obstacle. Further, it was pointed out that once users become familiar and comfortable with certain functions of a system (e.g. word processing), a strong tendency exists to quickly forget that such a system was not designed or intended to be used for processing/communicating sensitive material. It was also noted by some that while present users of office automation systems may be unsophisticated, the next wave of employees will contain many sophisticated users in all areas of government operations increasing the potential for misuse and the need for built-in security measures.

The fact that office automation is an integrative technology seems to be generally recognized. At the same time, uncertainty exists as to whether data security questions arising out of office automation are analogous to those of word processing, EDP, communications or even paper records. It was suggested that security elements of each of these could apply to office automation but that office automation because of its user-friendly communications (and portability) gives rise to a number of new concerns. It was noted that with respect to office automation ensuring that confidentiality of sensitive information is maintained is much

more than just a technical question. Of equal importance is the need to develop practical and pragmatic operating procedures for daily user which cover, aside from technical security features of the systems, areas such as the handling of diskettes and print-outs, the purging of memory, the handling of passwords and encryption, etc.

There was general agreement by those with technical and operational expertise in computer/communications technologies that if appropriate data security features are not taken into account in the early stages of the design of office automation systems and the development of functional specifications, it is generally much more costly to undertake a retrofit at a later date. The DOC field trial includes the use of portable intelligent terminals or microcomputers. Such use increases data security concerns and must include a review of the additional risks involved.

For the past three decades, the federal government has had a security policy and extensive experience and practice in protecting national security information against unauthorized disclosure. Although there is general consensus that the security policy of 1956 is dated and needs to be reworked both in terms of new information technologies and new information legislation, many of the principles expressed in the policy are still applicable. Similarly, in the area of information management policy, the federal government has developed policies on access and use of information, the use of various information technologies, and the day-to-day management of recorded information. Many of these policies contain elements which address security concerns. Office automation encompasses or involves all aspects of information technologies and information management including security.

While the federal government does have data security criteria and standards which have to be met before computer and communications equipment can be used to handle classified information related to the national interest, there are currently no specific, practical and comprehensive criteria for handling "sensitive" (non-national security interest)

information in various types of automated office environments. Such criteria are urgently needed. Since an inherent objective of office automation is to increase the effectiveness of decision-making throughout an organization, there will be a need to be able to put "sensitive" information on the systems. In order for office automation systems to be able to be used in as wide a range of application areas as possible in the federal government, such systems and accompanying procedures must be able to meet legal and federal administrative information policy requirements on information access and use.

There is no doubt that curent and new administrative policies of the federal government on the use of various information technologies and on informatic management, including those arising from the requirements or the Access to Information and Privacy Acts, do apply to information in office automation. However, because office automation is a new integrative technology, there appears to be a need for a pilot project to address the application of the government's new information management policies when using this technology. For exampe, one of the useful tools which needs to be developed is a matrix of types of information exempted from disclosure under the Access to Information and Privacy Acts, whether the exemptions are mandatory or discretionary, whether the class or injury test applies, whether consultation with others is necessary, etc.; also such a matrix needs to be translated into specifications for office automation systems for use by the government.

There appears to be a need to develop a practical set of guidelines, procedures and practices which would ensure that the use of the new information technologies in the federal government is in full compliance with existing legal requirements and new information policies, especially in matters pertaining to ensuring the security of sensitive information. The development of this set of guidelines, procedures and practices for office automation systems for non-national interest but still sensitive information would be an exercise in application, in an

integrative sense, of existing government policy, directives, standards and guidelines on information processing and communications to office automation systems.

The Department of Communications is a leading agency in office automation systems development. Also, the OCS field trial at DOC involves the use of portable microcomputers while the area of application involved is a policy area and the Minister's office, i.e. an area where sensitive information is being handled. For these reasons and because of the role of the Department in the high technology fields of electronic information processing and communications including communications security, it would appear relevant for DOC in conjunction with other appropriate government bodies and private sector representation to undertake a pilot project for addressing, in a practical sense, data security concerns arising from the use of office automation systems.

The payoffs to an organization in adopting office automation systems are in the areas of productivity improvements and increasing the effectiveness of the decision-making process. While office automation as a productivity tool for handling routine information flows offers limited returns on investment, harnessing it as a decision-support mechanism offers much greater payoffs to an organization. However, to be able to serve as a support mechanism for effective decision-making, an office automation system must be able to handle sensitive information and have features which assist in ensuring that data security requirements are met.

Consequently, the size of the market and rate of market penetration by Canadian suppliers of office automation equipment is directly related to the degree that Canadian-made systems are able to handle sensitive information. This is especially true for the public sector market in Canada and the U.S. which must abide by the requirements of various information laws.

In order for Canadian suppliers of office automation systems to have access to the widest possible markets in the federal public sector, their systems must be able to meet the data security requirements of the federal government including those arising from the Access to Information and Privacy Acts. Further, since many of the requirements of federal information legislation are analogous to the needs of the private sector and there is a trend in the private sector towards the adoption of rights and protection of personal information, it is imperative that Canadian suppliers be made aware of this as soon as possible.

Consequently, high priority should be given to preparing a document for Canadian suppliers of office automation systems which will translate, in clear and basic terms, the requirements of the Access to Information and Privacy Acts and the data security concerns of the federal government so that these can be built into their product offerings. Such a document should also demonstrate the linkage between present federal government data security requirements and those of the market both in Canada and abroad.

This report does not purport to be an all-inclusive review of security, confidentiality and privacy issues and concerns arising out of the introduction of office automation in the federal government. Such a study would necessitate much more time and the scope could be too extensive. This report is thus more in the nature of the preliminary overview of areas of concern. Nevertheless, it is clear that once the OCS field trials have met their technical objectives and one has learned to cope with key ergonomic concerns, questions related to information content and data security must be addressed.

VII. POST SCRIPTUM

Since the completion of the 1984 Data Security Report, a number of events and activities have taken place related to security, confidentiality and privacy (SCP) concerns.

First of all on 15 December, 1985, a series of amendments to the Criminal Code became law. Included were two specific amendments pertaining to computer crime and data abuse. Together with existing sections on telecommunications crime, these two amendments do appear to provide adequate protection and redress for any unauthorized use of computer/communication/information technologies and data/software content. A detailed review of these new amendments is presented in a publication also available at the CIIEL titled Legal Issues in Integrated Information Systems: An Overview of Practical Considerations and Recent Developments.

Secondly, the 1984 Data Security studies brought to the fore the fact that "information law" was a major source for both data security concerns and data security requirements. It was also discovered that the linkages between information law and information management (including SCP aspects) were not well understood or appreciated. Consequently, a series of studies were undertaken to address this deficiency resulting in the above noted Legal Issues report. In addition to the Criminal Code, this report also reviews SCP concerns arising out of the Evidence Act (e.g. admissibility of computer-generated records, authentication, etc.), Access to Information and Privacy legislation, Copyright and records retention requirements (e.g. should these be changed to allow for computerized record-keeping)?

In this context, it should be noted that the Parliamentary Committee which reviewed the first three-years of operations of the Access to Information and Privacy Acts recommended in its 1987 report that the federal government incoporate in the Privacy Act certain data security measures.

Specifically, the Committee recommended "the establishment of apropriate administrative, technical and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or jeopardy to their security or integrity..." (Recommendation 5.25, p. 28). The provincial Privacy legislation of Quebec already contains similar requirements.

The third major activity following the 1984 Data Security report has been the commissioning by the Department of Communications of a survey and study to determine private sector user requirements for security, confidentiality and privacy in integrated office systems and information interchange. Undertaken by Stevenson Kellogg Ernest & Whinney, Management Consultants, and supported by Thorne Ernest & Whinney, Chartered Accountants, and Infoman Inc., Information Policy and Management Consultants, the purpose of the study is fourfold:

- to determine, through literature reviews, surveys and focus groups, private sector (i.e. non-government) requirements for privacy, security and confidentiality in office automation systems;

- to determine whether the change from paper to "electronic" documents in integrated office systems is generating new or different issues and a different set of system requirements;

- to develop a statement of user requirements that could be used by individual vendors and organizations in considering product development and use; and,

- to have the results of the study serve as part of the Canadian input to the development of security-related standards by the International Standards Organization (ISO).

These surveys and studies are scheduled to be completed by Fall, 1987.

Fourthly, it should be noted that the Canadian Workplace Automation Research Centre (CWARC) and the Public Archives of Canada are sponsoring a project which will lead to the development of "Functional Specification for Electronic Document Management in Integrated Office Systems (ISO)". A working group composed of representatives and experts from key federal agencies as well as industry plans to issue a set of "draft" specifications for summer, 1987. Of interest from a "data security" perspective is the fact that a substantial number of these functional specifications will address questions of access and confidentiality, classification, privacy, protection and conservation of vital data, access and use control features, etc.

Finally, since 1984 the federal government has undertaken a major review of its security policy. The result was the issuance 18 June, 1986 by the Secretary of the Treasury Board of a new "Security Policy of the Government of Canada" along with a set of "Security Policy Implementation Guidelines" on 11 August, 1986.

The new Security Policy has a number of features which are worth noting, namely:

- it basically takes a technology-free approach to the protection of "information" and provides a general management framework and standards for protection across government; and,

- the introduction of two basic types of security classifications; the first set of classifications is for information pertaining to the national interest. Included here are the classifications of,

TOP SECRET - to prevent <u>exceptionally grave injury</u> to the national interest,

SECRET - to prevent <u>serious injury</u> to the national interest,

CONFIDENTIAL - to prevent <u>injury</u> to the national interest.

The designation of RESTRICTED has been dropped and may only be assigned in relation to RESTRICTED material received from NATO or the OECD.

The most significant aspect of the new security policy is that it seeks to reduce the amount of material requiring classification. It does so by introducing a new category of protection for "sensitive" information. (This is along the lines suggested in the 1984 Data Security Report.) The new security policy introduces the category of "PROTECTED" information" which applies to information which requires enhanced protection but which lies outside of the national interest. Examples of PROTECTED information include that which is exempt from access under specific provisions of the Access to Information and Privacy Acts (e.g. personal, third party, law enforcement and investigation information). Such information will be protected by limiting access to persons having a "need to know".

As such, it may well be that the data security requirements in integrated office systems for "PROTECTED" information in the public sector match those required in general by the private sector.

It will also be very interesting to know to what degree the Canadian situation is similar to or different from those in other countries. Comments from those attending the CIIEL on data security and related matters in integrated information systems are therefore most welcome.

REFERENCES

The following is a short list of references utilized, other than those already noted in the report itself:

1. The Electronic Office of Canada, Department of Communications Canada, May 1982, 40 pages.

2. Trying Out the Future: Office Communications Systems in the Federal Government, Department of Communications, Spring 1984, 25 pages.

3. Electronic Data Processing Security Standards and Practices for Departments and Agencies of the Government of Canada, Government EDP Standards Publication GES/NGI-14, June 1980 (under revision).

4. Knoppers, Jake V. Th., Report on Vulnerability Issues, Interdepartmental Task Force on Transborder Data Flows, Department of Communications, December, 1982, 102 pages.

5. Knoppers, Jake V. Th., Report on Possible Security/Confidentiality Implications of the Application Areas and Information Content of the OCS field trials, prepared for the Security Programs and Operations Division, Department of Communications, March 1984, 29 pages.

6. Knoppers, Jake V. Th., Report on Key Federal Information Legislation and Information Policies which Impact on Possible Security/-Confidentiality Implications in the OCS Program, prepared for the Security Programs and Operations Division department of Communications, March 1984, 47 pages and appendix 22 pages.

7. Knoppers, Jake V. Th., Security Confidentiality in the Electronic Office: A Preliminary Review of Issues and Concerns in the Federal Government Sector, June, 1984, 38 pages.

8. John McDonald, Interim Report of the PAC/DOC Information Management working Group, Public Archives of Canada, June, 1984, 62 pages and appendices.

9. Open and Shut: Enhancing the Right to Know and the Right to Privacy, Report of the Standing Committee on Justice and Solicitor General on the Review of the Access to Information and the Privacy Acts, Ottawa, March, 1987, 130 pages.

10. Government Security Policy, Circular No: 1986-26. Secretary of the Treasury Board, Ottawa, 18 June 1986, 22 pages plus appendices.

11. Security Policy-Implementation Guidelines, Circular No: 1986-41. Secretary of the Treasury Board, Ottawa, 11 August 1987, 45 pages.